AITKEN LAMBERT ELSWORTH

CHARTERED ACCOUNTANTS (S.A.)

With Compliments

5A Rydall Views
Rydall Vale Office Park
38 Douglas Saunders Drive
La Lucia Ridge, 4051

Tel: 031 202 7601
Tel: 031 277 2740
Fax: 031 202 7663
Email: info@aitkenlambert.co.za
Website: www.aitkenlambert.co.za

Directors: CC Elsworth, A King, E Pillay and AG Wiggill

CA(SA) CHARTERED ACCOUNTANT SOUTH AFRICA

[Forward email](#)

KEEPING YOU IN TOUCH

CA(SA)DotNews

In this Issue

May 2024

Your Employer Annual Declaration is Due by 31 May

"Failure by an employer to comply with its obligations does not only harm that employer and the fiscus, but also employees. SARS vigorously pursues employers that fail to comply." **(SARS)**

Employers must submit their annual reconciliation declarations (EMP501) with accurate and up-to-date payroll information about their employees by 31 May this year.

Subscribe

This is among the requirements imposed on employers by the Fourth Schedule to the Income Tax Act:

- deducting or withholding employees' tax from remuneration,
- paying the above to SARS monthly before the 7th of the following month,
- reconciling employees' tax during the annual and the interim reconciliation, and
- issuing tax certificates (IRP5s/IT3(a)s) to employees timeously.

A SARS focus area

The employer-reconciliation process is a focus area for SARS, not only to ensure compliance among employers, but also because it enables SARS to issue individuals with income tax auto-assessments.

SARS uses the IRP5/IT3(a) certificate information submitted by employers through the annual reconciliation process to prepopulate the employees' annual income tax returns (ITR12), and employees cannot change this information.

This means the employer-reconciliation process is also a key phase in the Income Tax Filing Season, because incomplete or incorrect information will make it difficult for employees to fulfil their tax obligations and because employees require IRP5 and IT3 certificates to file their income tax returns in time during tax season.

As such, SARS says it vigorously pursues employers that fail to comply and, where necessary, aims to make tax non-compliance hard and costly through hard enforcement, for example, court action, asset seizure and criminal prosecution.

What needs to be done?

- Register employees who are not registered for income tax.
- Review the year's EMP201 declarations that declare the total tax liability for each tax period for:
    - Employees' Pay-As-You-Earn (PAYE) tax,
    - Unemployment Insurance Fund contributions (UIF),
    - Skills Development Levy (SDL)
    - Employment Tax Incentive (ETI) amounts (if applicable).
- Submit any outstanding monthly declarations (EMP201) and settle all payments due to avoid administrative penalties for non-compliance or late submission, and to reduce interest charges on delayed or outstanding amounts.
- Ensure the values on the EMP201 declarations and on the tax certificates balance to the actual payments made to SARS.
- If any discrepancies are identified in the EMP201 declarations, these must be corrected when submitting the EMP501.
- The EMP501 Annual Reconciliation Declarations must include:
    - Monthly employer declarations (EMP201).

- Information about payments made (excluding penalties and interest paid).
- Employee tax certificates (IRP5/IT3(a) generated) covering the tax year from 1 March 2023 to 29 February 2024.

- Monitor the status of your submission to ensure the EMP501 has been successfully filed with SARS - a submission rejected as incomplete or due to a data error is considered *not* to have been submitted, and the taxpayer will be liable for non-compliance penalties.
- Keep accessible employer records with a register that contains each employee's personal details and financial records as prescribed by the Commissioner for at least five years.
- Also complete the interim reconciliation process in September/October each year to enable an easier and more accurate annual reconciliation submission and an up-to-date employee database.

Consequences of non-compliance

- ETI refunds (unused ETI amounts) can only be claimed by submitting interim and annual reconciliations (EMP501s). Failure to do so will result in ETI refunds being forfeited.
- Submitting an incomplete EMP501 or submitting an EMP501 after the due date will result in administrative penalties, amounting to 1% of the year's PAYE liability. This penalty increases by 1% monthly, reaching up to 10% of the year's PAYE liability. A penalty assessment notice (EMP301) will be issued. It is possible to incur two penalties for the same period i.e. both a PAYE late payment penalty and PAYE administrative penalties.
- In addition, it is a criminal offence for an employer wilfully or negligently to:
  - Fail to submit full and complete EMP201 or EMP501 returns to SARS by the due date.
  - Fail to issue an IRP5 or IT3(a) certificate to an employee within the specified periods.
  - Fail to deduct or withhold PAYE or UIF, or not to pay any PAYE or UIF deducted or withheld over to SARS as required by law.
  - Use or apply PAYE deducted or withheld for any purpose other than to pay that amount to SARS.

  Any person found guilty of one of these offences is liable, on conviction, to a fine or imprisonment for up to two years.

We can help!

Let us help you review your employees' tax obligations and prepare for submission of the Annual Reconciliation Declaration. Similarly, if penalties and interest have already been imposed on your business, we can assist in requesting remission from SARS.

How and When to Save a Struggling Start-Up

"Failure is simply the opportunity to begin again, this time more intelligently."- (Henry Ford, founder of Ford Motor Company)

Data from StatsSA has shown that more than 1,500 businesses closed their doors for good in South Africa last year. This can come as no surprise to anyone who conducts business in South Africa at the moment, with spiralling costs, high interest rates and other tough market conditions that include frequent load shedding at short notice.

It is therefore highly likely that all business leaders will go through tough times and for those with start-ups they can often seem insurmountable. If your start-up is one of those failing businesses the first thing you need to do is determine if the company is worth the extra energy, investment and effort required to save it, and if the answer is yes, then take our steps below to ensure that happens.

Save or close?

The first step to deciding whether to save a company is to work out the root cause of the troubles. Often this will take a team of outsiders, but a conversation with us as your accountants should be the first step. We can help you quickly assess whether your troubles come from external issues such as competition, market conditions or new regulations, or whether they are from internal issues such as poor management, a high level of debt, bad hires or inadequate equipment.

Next you need to be brutally honest with yourself. What was it that made you enter the market? What made you unique? Are these things still true? Is your product obsolete? And is your business still capable of turning a profit? Assuming you believe profit is still achievable, then the next step is a full evaluation of the finances, from assets to debits and invoices outstanding, so you can find out just how bad things are.

From there, we can help you work out the costs of necessary adjustments. Do you need restructuring? New equipment? Or new staff? What will it cost to fix, and do you have the ability to go through the necessary changes? You will need to carefully consider all these steps. You have invested a lot of effort and emotion into this company, and making these decisions rationally can therefore be hard. Having brought advisors onboard, you now need to actually listen to what they have to say.

If you have completed all the steps before this and still want to go on, then ask yourself one final question. Are there alternatives? Is there anyone who would buy the company? A competitor who might consider a merger? And why would one of these options not be better than you keeping things going? It is important to consider all of these options, so that when you commit you know you are on the right path. If, after all of this, you are still determined to save the business, here is what you need to do:

- **Rank your challenges**

  Being in a start-up can be overwhelming. It's likely you have more than one challenge that's driving your company into distress, and you may not know where to begin. Your first step should be ranking your challenges. Which of your challenges are the most dire? Is debt getting on top of you

each month? Is someone stealing from your inventory and causing you a loss? By ranking your difficulties, you can see which are the most urgent fixes and can tackle them in order, knowing that each tick on the list is a step closer to saving the company. Fixing everything, starts with fixing one thing.

- **Consolidate debts**

  Debt consolidation or restructuring can help your company save a great deal simply by lowering the interest payable each month. By consolidating debts into one loan or restructuring loans with different interest terms you can both pay them off quicker and save on the monthly expenses.

- **Find the funding**

  Whether your challenge is a lack of advertising, a glut of debt or broken equipment, the answer is often funding. Whether you need to sell a percentage of the business, withdraw money from your own savings, take a loan or beg for money from friends and family, addressing the lack of funding and attending to these challenges is a necessary step. We can help you determine the best way to use the funds you have to make the biggest impact.

- **Re-evaluate your business plan**

  Take a look at your business blueprint and particularly your projections for the future. Now, contrast it with the present state of affairs. Which projections did you get right, and which failed? Why? Has there been less demand than expected? Did your marketing team maybe direct their efforts at the wrong audience? What has your customer retention been like? Which expansion opportunities did you miss, and where did you stray from the original plan? Regardless of the root cause, it's now time to sit down with the experts and brainstorm a solution or a substitute that can fix these issues.

- **Maximise your staffing**

  It's an old and much-repeated adage for a reason, "A company's best asset is its staff". Take a look at your staffing and truly analyse whether the people involved are the right fit for their roles. Do they all have the training necessary to do their jobs to the best of their ability, and are they motivated to do so?

  Depending on the size of your staff it may help to meet with each employee, to ask them what they need and what they think is missing. Often employees may offer insights that can be missed at the top level. Making sure everyone is given the skills they need, feels valued and understands their role will be essential if you want to save your company.

  Just as important is making sure that those who are hired by your business are all offering value. If your company is struggling, then it is not the time to keep someone on who cannot perform or be retrained to fill a more beneficial role. Many roles these days can be outsourced to freelancers where you only pay for the work that is done. Carefully consider which roles may benefit from this.

- **Overhaul your sales techniques**

  Many business leaders have underestimated the extent to which the sales process has changed over the past few

years. There are a lot of new ways of engaging with customers and making new connections, and these should all be actively utilised if you want to be successful.

From social media to remote selling and data-driven sales, there are new ways to get the most from your sales professionals. Customer Relationship Management (CRM) systems allow your staff to track and analyse customer behaviour, better targeting the client's needs. If your competition is making the most of these sorts of strategies and you are not, then it's time to rethink the way you close the deal.

Don't give up

Turning around a business can be emotionally draining and thankless work. Now that you have done the evaluation and committed to fixing things, this is not the time to give up. Each time you tick off one of your list of challenges is a step closer to success, and **as Steve Jobs always said, "I'm convinced that about half of what separates successful entrepreneurs from the non-successful ones is pure perseverance."**

Beneficial Ownership Registers - Now Mandatory with CIPC Annual Returns

"It is imperative that ALL companies and close corporations ensure compliance with the beneficial ownership filing requirements, to ensure good corporate governance and business continuity." **(CIPC)**

Following changes to the Companies Act on 24 May 2023, company directors and members of close corporations are obliged to lodge and maintain a detailed Beneficial Ownership (BO) Register, along with a list of supporting documents with the CIPC (Companies and Intellectual Property Commission). This register and documents must also be kept up to date within tight timelines and verified annually.

Pre-existing companies with their anniversary date after the promulgation of the amended Companies Regulations were required to file their beneficial ownership information with their annual returns. Registers for new companies and amendments must be lodged within 10 days. **This means that all entities in CIPC's register must have filed their beneficial ownership information by 24 May 2024** – one year since it became mandatory.

The Commission, citing a huge number of non-compliant entities that are yet to file their beneficial ownership and/or securities register information, is enforcing compliance by implementing more serious consequences.

Consequences of non-compliance

- A new "hard-stop functionality" has been implemented by the Commission. That will prevent any non-compliant entities from filing their annual returns, which brings its own consequences.
    - The late filing of annual returns will incur penalties.
    - Banks, service providers or customers often require businesses to have up-to-date annual returns before engaging in business.
- The Commission will take further and necessary enforcement actions with regards to entities which continue to be non-compliant, such as:
    - investigation into the administration and governance processes of non-compliant business,
    - issuing of compliance notices; and/or
    - referral for deregistration and even final deregistration due to non-compliance.
- It is also a criminal offence to submit false or incorrect information to the CIPC.

What is required for compliance?

- Identify the beneficial owners of a company – these are individuals/natural persons who, directly or indirectly, ultimately own 5% or more of the company, or exercise effective control of that particular company.
- For each beneficial owner identified, collect the following:
    - full names, date of birth, correctly certified copy of ID or passport;
    - business or residential and postal address;
    - email address;
    - confirmation as to the participation and extent of the beneficial interest;
    - supporting documents.
- Collate the information in a register, which must be filed with CIPC, and upload the supporting documents to CIPC's website.
- Keep the register up to date, with changes filed with CIPC as soon as practically possible, but no later than 10 business days after notification.
- An updated register must also be submitted with the annual returns each year.
- The information must be treated as confidential and adequate precautions must be taken to prevent theft, loss, damage, destruction and falsification.

Top tip for hassle-free compliance

Our assistance will prove invaluable in ensuring your business remains compliant with both CIPC's beneficial ownership

requirements and annual return requirements, particularly following the hacking of the CIPC website and the problems and delays that followed.

We can also guide you through the complexities of CIPC compliance, manage the tedious processes and take care of the ongoing maintenance requirements, thereby eliminating your risk of non-compliance, which constitutes an offence and can incur administrative penalties.

Five Things You Need to do After the CIPC Hack

"The Internet is a worldwide platform for sharing information. It is a community of common interests. No country is immune to such global challenges as cybercrime, hacking, and invasion of privacy" – (Lu Wei, the head of the General Office of the Central Leading Group for Internet Security and Informatization from August 2013 to June 2016)

On the 1st of March 2024, the CIPC admitted it had been hacked. The CIPC said in a statement that, "Our ICT technicians were alerted, due to extensive firewall and data protection systems in place at the CIPC, to a possible security compromise and as a result, certain CIPC systems were shut down immediately to mitigate any possible damage."

While they referred to the incident as "an attempt" to hack their systems they also added, "Unfortunately, certain personal information of our clients and CIPC employees was unlawfully accessed and exposed."

A few days later MyBroadband.co.za said they had been contacted by the hackers who allegedly proved they had access to the site since 2021 and the CIPC could be understating the damage done. Whether the claims made to MyBroadband are accurate or not, the possibility this hack has leaked private information from many or all of South Africa's registered businesses and presumably given outside access to company registrations which potentially allows the hackers to make alterations to core business areas.

Together with a long-standing issue at SARS that periodically sees clients receiving an email or SMS stating, "unauthorised changes were made to your personal details on eFiling", it is clear that South African businesses need to be aware of the risks of online attacks at key government organisations and more importantly, know what to do about them.

These are the main concerns:

Private information leaked

According to reports, the hackers may have gained access to the private credit card information used to make payments to the CIPC. MyBroadband quotes the alleged hackers as saying the CIPC was "processing and storing credit cards in the clear." While most banks require access to an app as verification, the exposure of CVVs and expiry dates of cards is a risky proposition. When combined with

other information stored on the site, such as the names, addresses and signatures of directors there is a real risk that company clients and contacts may be open to being scammed through fake profiles or other contacts generated by malicious third parties.

Access to Company registrations

If, as is alleged, hackers have gained unfettered access to the company registrations section and the login details for multiple clients, companies risk potential changes in their core information. Directors can be changed, addresses altered and critically, key documentation can be downloaded.

The latter is of great concern as these documents could allow a fraudster to open bank accounts in a company's name. After that it becomes simple to contact clients saying that bank account details have changed, and even offer them the proof that they are speaking to legitimate company representatives. From there money could easily be siphoned into these phoney accounts and it may take weeks or even months to uncover.

What should you do?

With every company vulnerable it's critical to take a number of steps immediately to mitigate the risk and potential damage.

1. **Check bank accounts and cards**

   Monitor your bank account and card transactions even more closely than before for any signs of suspicious activity. If any unusual activity does occur, report the incident to the bank immediately and consider cancelling any bank cards that may have been exposed on the CIPC website and ordering new ones.

2. **Warn your clients**

   You may want to consider adding a warning to emails and client correspondence that asks them to treat any notices supposedly from your business of changes to bank account or personal details with caution due to the CIPC hack and SARS login leaks. The warning should carry the caveat that should they receive any bank detail change correspondence they should check with you directly before making alterations to payments.

3. **Change your usernames and passwords**

   Change all login details. Assume your current passwords have been compromised and check whether you have used them on other sites as well. Even if this is not the case, it's wise to change all your important passwords periodically, particularly those for bank accounts or other financial institutions.

4. **Warn your employees**

   Alert all employees that any emails, calls or other communication from banks, insurers or fraud divisions should be treated as suspect. Instruct your employees to authenticate communications directly with those departments immediately (using contact details they know to be genuine) rather than give away any information to an unverified person. This is good practice anyway in light of surging cyberfraud generally, but the CIPC hack makes it essential.

5. **Remain vigilant**

   We as your accountants are happy to help advise you on

how to monitor the credit bureaus and banks to track any illegal accounts, which may be opened in your name and discover suspicious changes in the invoicing and payments. A client who usually pays regularly suddenly stopping is now cause for an immediate follow-up.

Don't stop being cautious. These sorts of hacks can often come back to haunt a company months after they happen. Assume you will need to be careful for at least a year as the hackers work their way through their haul and try to make the most of it.

Your Tax Deadlines for May 2024

- 07 May - PAYE submissions and payments
- 24 May– Value-Added Tax (VAT) manual submissions and payments
- 30 May – Excise duty payments
- 31 May – VAT electronic submissions and payments, & Corporate Income Tax (CIT) Provisional Tax payments where applicable.

Note: Copyright in this publication and its contents vests in DotNews - see copyright notice below.